EL DELITO DE INTERCEPTACIÓN DE DATOS INFORMÁTICOS EN EL ORDENAMIENTO JURÍDICO COLOMBIANO: INCONVENIENTES EN SU TIPIFICACIÓN Y APLICACIÓN.

MIGUEL ÁNGEL SUAREZ FONSECA

ESTUDIANTE

TUTOR

MG. GIOVANNI ALCIDES MONGUÍ MERCHÁN

ESPECIALIZACIÓN EN DERECHO PENAL Y PROCESAL PENAL

UNIVERSIDAD SANTO TOMAS

SECCIONAL TUNJA

2021

Contenido

EL DELITO DE INTERCEPTACIÓN DE DATOS INFORMÁTICOS EN EL ORDENAMIENTO JURÍDICO COLOMBIANO: INCONVENIENTES EN SU TIPIFICACIÓN Y APLICACIÓN.

Miguel Ángel Suarez Fonseca

Resumen

Las nuevas tecnologías de la información en los últimos tiempos han tenido una exponencial inmersión en el ámbito del Derecho, principalmente en el campo Penal, contexto propiciado por el inminente auge de la globalización en todo el mundo, fenómeno que ineludiblemente permeo a Colombia trayendo consigo un nuevo reto jurídico -social que obligó la expedición de la ley 1273 de 2009, norma que buscó la protección e integridad de los datos informáticos y el afrontamiento de los desafíos y particularidades de este nuevo paradigma delictivo en nuestro país, aun así, se presentan problemas de tipificación y aplicación que se manifiestan en el delito de interceptación de datos informáticos contemplado en el artículo 269C del Código Penal Colombiano, ya que este tipo penal deja varios interrogantes al determinar los alcances que tiene el sujeto activo para incurrir en el delito con la expresión "sin orden judicial previa", situación que la Corte Constitucional aclara, manifestando no solo la necesidad de obtener orden judicial previa, sino además la de carácter posterior para no incurrir en su comisión.

Palabras Claves

Derecho, Tecnología, Delitos informáticos, Globalización, Interceptación, Datos informáticos.

Abogado, Universidad Santo Tomás Seccional Tunja, Candidato a especialista en Derecho Penal y Procesal Penal por la Universidad Santo Tomás Seccional Tunja, correo electrónico: miguelsuarez12@hotmail.com, móvil: 3137072110

Abstract

The new information technologies in recent times have had an exponential immersion in the field of law, mainly in the criminal field, a context propitiated by the imminent rise of globalization worldwide, a phenomenon that inevitably permeated Colombia bringing with it a new legal-social challenge that forced the issuance of Law 1273 of 2009, a rule that sought the protection and integrity of computer data and the confrontation of the challenges and peculiarities of this new criminal paradigm in our country, even so, there are problems of typification and application that are manifested in the crime of interception of computer data contemplated in article 269C of the Colombian Penal Code, since this criminal type leaves several questions when determining the scope that the active subject has to incur in the crime with the expression "without prior judicial order", a situation that the Constitutional Court clarifies, stating not only the need to obtain prior judicial order, but also the subsequent one in order not to incur in its commission.

Key words

Law, Technology, Computer crimes, Globalization, Interception, Computer data.

INTRODUCCIÓN

El mundo ha atravesado a lo largo de su existencia por grandes cambios culturales, sociales y estructurales a raíz de los distintos avances que el ser humano ha logrado aplicar y aprender con las distintas vivencias que recoge día a día, situación que sin lugar a dudas ha hecho que a todas las tareas y actividades del hombre le sean añadidas más herramientas para ser realizadas de manera fácil y ágil.

El derecho, no ha sido ajeno a todas estas manifestaciones de desarrollo y avance, principalmente en cuanto a su forma de ser ejecutado o vulnerado, es así que, con la aparición de los primeros registros de datos personales manuales, mecanográficos e incluso de los primeros computadores, se empezó a discutir sobre la seguridad de los datos almacenados en dichos registros y dispositivos, emergiendo así los delitos en los que se obtenían los mencionados datos con fines económicos.

Con el inminente auge de la globalización, el cual vino de la mano con otro gran fenómeno informático, como lo fue el internet, decantaron en que el mundo análogo y manual quedara atrás y emergieran como protagonistas la virtualidad y lo digital, con lo que claramente se eliminaron las barreras locales y transnacionales que separaban al mundo, pero que por otro lado, y observándolo desde el punto de vista jurídico, propiciaron un espacio ideal para que los delincuentes tradicionales replantearan su actuar delictual, ya que no había necesidad de acudir al entorno físico, pues desde cualquier lugar se podría materializar un delito, teniendo adicionalmente como punto a su favor el factor del anonimato que por lo general cobija a la red de internet, en ese sentido, con la tipificación de los delitos informáticos en el ámbito Colombiano con la promulgación de la ley 1273 de 2009, se vislumbra el esfuerzo por buscar la protección e integridad de los datos informáticos que a diario se movilizan por internet, pero que en otros casos resultan insuficientes como ocurre en el caso del delito de interceptación de datos informáticos dispuesto en el artículo 269C del Código Penal, en el entendido que su

descripción típica se torna confusa al no determinar el alcance concreto respecto del sujeto activo en la expresión “sin orden judicial previa”.

PLANTEAMIENTO DEL PROBLEMA

El fenómeno de la globalización en los últimos tiempos ha tenido un gran impacto sociológico, el cual ha estado vinculado con la eclosión de la informática, que eliminó las barreras temporales y espaciales de la vida del individuo, transformando la razón en imagen y reemplazando lo real por lo virtual.

Una globalización que no necesariamente funciona objetivada, es decir fuera del individuo, sino que principalmente desde dentro de él, desde su disposición afectiva, desde su propio modo de pensar, conceptualizar y racionalizar el mundo, llevándonos a entender entonces que el principal peligro que encierra la globalización es el tipo de pensar que le enmarca, la cual se encapsula en una sola vía de manifestación y desarrollo. Un pensar que es producto de la razón ilustrada devenida en razón tecno - científica. La globalización acaba con la experiencia moral; solo es posible la experiencia del instante, de la simultaneidad, del ya; la comunicación, para ser tal, debe ser informática, esto es, debe ser virtual, pero en tiempo real. De este modo, se reemplaza la realidad por la virtualidad, y en esa suplantación se olvida que todo ha sido un simulacro, y en ese olvido, el simulacro deviene en lo real, pues se olvida que se olvidó. La especie humana acorta los tiempos; "gana" tiempo, pero pierde el espacio, pierde la noción de distancia, esto es, de lejanía y de cercanía, teniendo como un claro ejemplo de esto las redes sociales, herramientas que han facilitado la comunicación de las personas, acortando distancias, permitiendo vivir experiencias del mundo real a través de la virtualidad. (Valdés Meza, 2009)

No obstante dentro de las múltiples ventajas que arribaron con el auge de las redes sociales, se desprende una cantidad inimaginable de información basada en opiniones o noticias que son expresadas por medio de estas plataformas como Facebook, Instagram y Twitter, etc., donde pueden aparecer las implicaciones que

rondan el ámbito penal, pudiendo dar lugar a los llamados cibercrímenes. (Jara Obregon, Ferruzola Gómez, & Rodriguez López, 2014)

La significación de cibercrímenes, se da en cuanto existe una relación directa entre el uso de las tecnologías de la información como lo pueden ser las redes sociales, con los derechos humanos y derechos fundamentales, la cual se traduce en la conjunción de buscar la protección de bienes jurídicamente tutelados por los ordenamientos jurídicos en el subsistema penal. (Carrillo, 2012).

Precisamente, el bien jurídicamente tutelado[2] que subyace dentro de esa relación jurídico-penal-digital, es el referente a la protección de la confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos, que se materializa en la comisión de delitos informáticos, en los que se realizan conductas u operaciones en las cuales se engaña al usuario que realiza compras por medio de su ordenador, se sustraen datos personales, mediante ofertas de trabajo falsas, se interceptan datos informáticos, etc. (Posada Maya, 2017)

De igual manera aparecen los delitos realizados por hackers, quienes entran de manera abrupta y sin ningún tipo de permiso a un sistema o a una red, con el fin de sustraer archivos o documentos y todo tipo de información privada de personas o empresas.

Por ultimo están los delitos que pueden a llegar a perjudicar la honra y nombre de las personas, mediante la publicación o divulgación de información privada, o realizando publicaciones que no tengan algún tipo de veracidad, o que siendo estas verídicas, ponen en la lustra publica a alguien. (Alvarez Pardo, 2017)

En nuestro país, según datos del Ministerio de las Tecnologías de la información y las Comunicaciones, en los últimos años existió un crecimiento exponencial de los usuarios que utilizan redes sociales como Facebook y Twitter, ocupando el primer

[2]Claus Roxin, lo considera como “circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema social global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del propio sistema”, y que para declarar una conducta como delito, no debería bastar que suponga una infracción de una norma ética o divina, es necesario ante todo la prueba de que lesiona intereses materiales de otras personas, es decir, de que lesiona bienes jurídicos. (Leyva Estupiñan, 2015)

y segundo lugar respectivamente, como las favoritas de la población colombiana, es así que “Facebook, en Colombia ocupaba el lugar número 14 a nivel mundial con más de 15 millones de usuarios y twitter 6 millones de usuarios, esta cifra pone a Colombia por encima en número de usuarios sobre países como Francia y Alemania". (Ministerio de las Tecnologias de Informacion y las Comunicaciones, 2020)

Datos que nos muestran indiscutiblemente que estamos ante la presencia de comportamientos que se materializarán cada vez más, por el consecuente apoderamiento que las Tecnologías de la Información y Comunicaciones van alcanzando en el ámbito social y económico, los cuales en la actualidad cobijan la mayoría de actividades que las personas realizan en su diario vivir.

Indica el profesor Ricardo Posada Maya, que las tecnologías de la información, ya no son una simple herramienta de comunicación, si no que con su irrupción, se han convertido en un objeto capaz de incidir en la misma realidad, ya sea de forma positiva, al desarrollar nuevas tecnologías y conocimientos, o al contrario de forma negativa, cuando se usa para la comisión de conductas punibles. (Posada Maya, 2017)

Ahora bien, es claro que el Estado Colombiano es el garante del cumplimiento de los derechos fundamentales y el encargado de ejercer el poder punitivo y de contera ejercer el Ius puniendi, sin embargo a pesar de los esfuerzos y avances significativos como la expedición de leyes penales que apuntaron a la protección de la integridad de los datos informáticos, aún se presentan dificultades en la persecución penal de los delitos informáticos, precisamente por la desregulación existente sobre determinados conceptos y distintas plataformas tecnológicas y principalmente por el carácter de anonimidad que existe en la internet, lo que genera que no exista un control verdadero y real por parte de las autoridades judiciales sobre cómo debe ser su uso y sus límites (Franco Reyes, 2017), por lo que a priori y como mecanismo de prevención, se insta a la comunidad que hace uso de los sistemas informáticos, que en la actualidad es la mayoría de la población, para que

dentro de este entorno se actué bajo parámetros de responsabilidad, autocuidado y comprensión de su alcance penal. (Alvarado Carmona, 2016).

Con este panorama es claro entonces que existen falencias en Colombia respecto a leyes de carácter sustancial y adjetivo. que sean efectivas para penalizar este tipo de conductas, situación que se suma a los problemas que se erigen en la descripción típica de algunos tipos penales, como el establecido en el artículo 269C del Código Penal Colombiano, referente a la Interceptación de Datos Informáticos, que trae consigo un gran interrogante frente al sujeto activo de la conducta, ya que el tipo penal determina la obligación del funcionario que realiza las funciones de policía judicial a lo largo de un proceso penal, de obtener orden judicial previa para realizar la respectiva interceptación.

No obstante, en pronunciamientos de la Corte Constitucional, se determina la obligación del funcionario de llevar ante el Juez de Control de garantías, los elementos materiales probatorios producto de la interceptación de manera posterior, cobijando a este tipo penal con una doble obligación dentro de su descripción típica, situación que no describe el tipo penal del artículo 269C del Código Penal al realizar su lectura.

Con todo esto, se plantea la siguiente pregunta de investigación.

PREGUNTA PROBLEMA

¿Qué inconvenientes se presentan en la tipificación y aplicación del delito de interceptación de datos informáticos en el ordenamiento jurídico colombiano? El citado problema jurídico se desarrollará con el siguiente

OBJETIVO GENERAL

Determinar cuáles son los inconvenientes qué se presentan en la tipificación y aplicación del delito de interceptación de datos informáticos en el ordenamiento jurídico colombiano.

OBJETIVOS ESPECÍFICOS

1. Describir las principales implicaciones de las nuevas tecnologías en el ámbito del Derecho Penal.

2. Establecer la configuración típica de los delitos informáticos en el ordenamiento jurídico colombiano.

3. Identificar y describir el tipo penal de interceptación de datos informáticos en Colombia.

4. Establecer las dificultades y contingencias en la configuración y aplicación del tipo penal de interceptación de datos informáticos.

El documento se encuentra enmarcado dentro de la siguiente

JUSTIFICACIÓN

El mundo de la Internet va en un camino rápido y creciente cada día más y su uso se da en gran mayoría de la población del mundo, situación que ha traído grandes ventajas en la manera de comunicar situaciones o hechos que ocurren a diario, pero también ha sido un foco para que se presenten riesgos para sus usuarios, esto por la facilidad en la comisión de delitos de diferente índole; como lo son contra el patrimonio o la imagen, integridad de los datos informáticos y la honra de los seres humanos. (Cea Jiménez, 2012)

En nuestro país, ese mismo incesante desarrollo de la Internet, ha hecho que los delincuentes enmarcados en el ideal clásico de los hurtos callejeros no sean los únicos protagonistas a la hora de cometer delitos, pues en la actualidad existe gran facilidad de adquisición en el mercado de cualquier aparato electrónico ya sea PC, Tablet, teléfono celular, etc. Y se cuente además con una conexión a una red de internet, que también es de muy fácil acceso por estos tiempos, el delincuente tiene el camino abierto para causar graves daños a los sistemas informáticos, ya sea que

se dirija contra una persona del común o a hasta grandes compañías que tienen bajo su cargo manejo de importantes recursos o posean información relevante que pueda poner en riesgo la integridad de la comunidad en general. (Posada Maya, 2017)

Ahora bien, a lo anterior podemos añadirle que la internet deja “espacios en blanco” usufructuados por los delincuentes, pues al iniciar el trasegar dentro de la red, esta permite actuar bajo parámetros de anonimato, abriendo la puerta a la impunidad, ya que no existen figuras férreas de control que permitan una identificación precisa del individuo que cometa delita en estos entornos digitales.

Dicha limitante del anonimato es la que más destaca, porque la identidad del victimario es una incógnita y si bien con el correlativo avance tecnológico existen mecanismos para ubicar sitios o lugares desde donde se utilizaron servicios web, es claro que es necesario la plena identificación de la persona que haya incurrido en las conductas lesivas. (Franco Reyes, 2017).

Otro punto importante de análisis es el elativo a que hoy en día la Tecnología y más aún la Internet, han hecho que nos veamos expuestos a gran variedad de riesgos, teoría que el jurista Alemán Ulrick Beck llamó la “Sociedad del Riesgo”, la cual plantea que la tecnología ha sido una fuerza poderosa capaz de influir en el desarrollo de la civilización, aumentado así las posibilidades de intervenir y alterar el mundo social, (Beck, 1986), fruto de eso es que a los clásicos riesgos tales como inundaciones, incendios, sequias, pandemias etc., se deben agregar ahora aquellos que son producto de la conducta humana, como por ejemplo los avances tecnológicos y de la informática. (Galindo, 2015).

Situación que podemos ver materializada en la crisis actual mundial en la que se conjugaron en el entorno social, el riesgo pandémico y el tecnológico, con la aparición del virus del SARS-CoV-2 (COVID -19), que bajo su estela trajo el aumento de comisión de conductas punibles en entornos virtuales explicado en la imposibilidad de salir a las calles, por el prolongado tiempo en que la población se encontró confinada en sus hogares. (León Felipe, 2020)

Basta con observar los datos entregados por la Fiscalía General de la Nación, en su direccionamiento estratégico en tiempos de COVID-19, en el que se indica que, desde el inicio del confinamiento en Colombia, el cibercrimen ha evidenciado un incremento significativo por el orden del 62% en comparación con el año 2019 que registró un total de 28.827 casos. Desde el 24 de marzo a la fecha del total de delitos cibernéticos denunciados se han recibido 6.453 por infracciones relacionadas con delitos informáticos, la protección de la información y de los datos, sumado al incremento de los delitos de suplantación de sitios web para capturar datos personales, la interceptación de datos informáticos y daño informático, a su vez "se han identificado 471 páginas web con contenido malicioso, malware, dedicadas a la captura de información personal, financiera y empresarial". (Fiscalia General De La Nación Colombia, 2020)

Es claro entonces, que con la aparición de la tecnología y sus distintas aristas, en todos los ámbitos de relación de la vida cotidiana, nace para la sociedad un potencial riesgo tecnológico, al no tener un conocimiento profundo sobre su alcance y el nivel de incidencia que este puede llegar a traer para las relaciones humanas. (Ramirez, 2009).

Y precisamente, dentro de esas relaciones humanas, es que se podrían ver enmarcadas conductas punibles que atenten contra bienes jurídicos, que a priori no han tienen gran relevancia dentro del pensamiento general de lo que es el Derecho penal como los homicidios, las lesiones, hurtos, estafas, etc., pero que el profesional del derecho, debe empezar a darle una mayor relevancia, pues como se ha explicado de contera ya, la tecnología vino para quedarse, y en un futuro no muy lejano este fenómeno repercutirá en que se tengan que replantear varias de las normas penales que hablan sobre delitos informáticos, enfocándose principalmente en el manejo de terminologías propias de la ciberdelincuencia. (Loredo González & Ramirez Granados, 2013)

Por lo tanto, este escrito, tiene como propósito brindar información ya sea a abogados, personas que trabajen investigando delitos informáticos y personas del común, sobre lo importante y necesario que es conocer el alcance que tienen el uso

de las TIC´S en algunas aristas de la interacción social y la responsabilidad que se debe mantener al usar internet como mecanismo de prevención general con el fin de garantizar que la comisión de ciberdelitos baje de manera considerable.

Por otra parte, el documento propende hacer un análisis del artículo 269C del Código Penal Colombiano, referente a la interceptación de datos informáticos, en el que se ilustrará como el tipo penal se queda corto al explicar los alcances que tiene el sujeto activo para incurrir en el delito, por lo que es necesario hacer el estudio de sentencias de la Corte Constitucional, con las que se aclara el camino interpretativo de este punible y como se debe analizar al término "sin orden judicial previa".

METODOLOGÍA

El enfoque de la investigación es Cualitativo[3], en la medida que se busca analizar las características de las nuevas Tecnologías de la información, precisando sobre todo conceptos técnico jurídicos que pueden llegar a aplicarse en el entorno del derecho Penal, conocer distintas concepciones de lo que es el delito informático, y realizar un estudio al tipo penal de interceptación de datos informáticos, explicando su conceptualización general, estructura y configuración, igualmente se examinarán que contrariedades podrían existir en su descripción típica.

La presente investigación es de tipo Jurídico-analítica-descriptiva, ya que busca analizar conceptos referentes a la relación entre el Derecho Penal y la Tecnología como este el desarrollo de este fenómeno ha incidido activamente en el comportamiento de las personas, además se busca estudiar la estructura típica del delito de Interceptación de Datos Informáticos, para observar que falencia presenta en su descripción típica y sus alcances punitivos.

En ese orden de ideas, una hipótesis para el problema planteado parte de la poca claridad existente en la descripción típica del delito de interceptación de datos

[3] Se puede definir la investigación cualitativa como el estudio de la gente a partir de lo que dicen y hacen las personas en el escenario social y cultural. El objetivo de la investigación cualitativa es el de proporcionar una metodología de investigación que permita comprender el complejo mundo de la experiencia vivida desde el punto de vista de las personas que la viven (Taylor y Bogdan, 1984). Las características básicas de los estudios cualitativos se pueden resumir en que son investigaciones centradas en los sujetos, que adoptan la perspectiva del interior del fenómeno a estudiar de manera integral o completa. (UJAEN.ES, s.f.)

informático, el cual deja un vacío a la hora de interpretar el término “sin orden judicial previa”, pues dicho presupuesto debe entenderse como una doble obligación para la persona que cumple con funciones de investigación en un proceso penal, es decir, no sólo se requiere orden judicial previa, sino además se requiere del control judicial posterior por mandato constitucional.

La Técnica de recolección de datos usada será la Bibliográfica, pues la información recolectada está basada en el uso de fuentes como las Normas Jurídicas, Sentencias y Doctrina que estén relacionadas con el tema y que permitan dar respuesta a la pregunta de investigación.

I. PRINCIPALES IMPLICACIONES DE LAS NUEVAS TECNOLOGÍAS EN EL ÁMBITO DEL DERECHO PENAL.

1.1. Derecho y tecnología

1.1.1. Derecho

La palabra derecho deviene del latín *directum*, lo cual significa no apartarse del buen camino, seguir el sendero determinado por la ley, lo que es bien dirigido. Derecho también puede ser definido como: “la ordenación de la razón para el bien común, dada y promulgada por quien tiene a su cargo el gobierno de la comunidad" (Naranjo Mesa, 2000); Y de ahí que la ordenación de la razón sirva para establecer el recto proceder de la conducta humana. En términos generales el derecho es el conjunto de normas jurídicas creadas por el estado para regular conductas externas de los hombres y en caso de su quebrantamiento devienen en una sanción judicial (Poder Judicial de México).

Para John Locke, el derecho se asemeja a lo *correcto*, es decir este autor considera que se tiene derecho a hacer cosas que o estén prohibidas por la ley de naturaleza, en ese entendido, los derechos pueden ser tomados como una libertad, pero sin que estos tengan un deber de otros más allá de la naturaleza y según esta ley de la

naturaleza, los hombres tiene el derecho de apropiarse del fruto de su trabajo, pero al no decir nada esta ley respecto a aquello de lo que tienen que apropiarse, en ese sentido los hombres tienen la libertad o el derecho de escoger que y como desean realizar esa apropiación, pero como el uso que Locke le da al término “derecho” se circunscribe sólo a lo no prohibido, esa libertad desaparece en cuanto se puede identificar en la ley de la naturaleza algún tipo de restricción. (Fernandez, 2011)

Por otro lado, Locke, se refiere al derecho o los derechos, como un poder moral, es decir, como una facultad que tienen los hombres de hacer lo que creen oportuno para la preservación de sí mismos y del resto de la humanidad, por lo que cuando se ejerce dicho poder moral se crean y modifican la situación de derechos y deberes de otros, como por ejemplo cuando alguien se apropia de determinado bien, crea derechos y deberes frente a los demás, prerrogativas que antes de esa apropiación moral no existían. (Fernandez, 2011).

De la anterior idea se decanta una relación existente del Derecho con la Tecnología, en la medida que ambas ciencias tienen su génesis a partir del poder moral que el ser humano aplica en cada una, pues en primer lugar el Derecho nace a partir de la necesidad y aptitud del hombre de apropiarse de ciertas cosas para lograr su subsistencia, creando así una creencia subjetiva y objetiva frente a sí mismo y a los demás, de que un bien ahora le pertenece.

De igual forma, la Tecnología tiene como punto de partida el poder moral que ejecutó el ser humano, al observar la necesidad de crear y aplicar nuevas herramientas que facilitaran las tareas que se realizaban día a día, una manera de sobrellevar y subsistir frente a las adversidades y peligros que la naturaleza y el mismo hombre generan al mundo.

1.1.2. Tecnología

La palabra Tecnología puede asociarse con maquinaria, o como equipo sofisticado, concepción que tiene un aspecto observable y funcional, es decir que puede ser

percibida y tocada físicamente como un teléfono celular o una pantalla de televisión, pero esta definición solo es una de las variantes que el concepto de tecnología presenta, y que además podría tornarse inequívoco. (Betancur, 1998).

Es por esa razón que el concepto de Tecnología como tal puede ser muy ambiguo y pueden existir gran variedad de definiciones, como la que ofrecen Westphal y Dahiman, que la definen como un método o procedimiento para hacer algo, concepto que es muy genérico y similar al que se mencionó en primera instancia (Dahiman, 1983).

En orilla distinta, Bertrand Nezeys plantea que la tecnología es una rama del saber, constituida por el conjunto de conocimientos y competencias necesarias en la utilización, mejor y creación de las técnicas, además que le da importancia al saber formal, proveniente de la ciencia, y al saber informal que deviene del trabajo diario y del conocimiento que forma pete de determinada cultura. (Nezeys, 1985)

1.1.3. Conjunción del derecho y la tecnología

No hay duda que los adelantos tecnológicos han transformado la vida de los hombres. La facilidad y versatilidad de las comunicaciones han ayudado a derrumbar barreras de espacio y tiempo, ya no importa la ubicación, la internet nos acerca con tanta inmediatez que en cuestión de segundos pareciera que la otra persona al lado de la pantalla está al frente de nosotros; pero dentro de ese acercamiento cada vez más amplio que nos brinda la red, se encierra un enigma sobre el alejamiento correlativo que este genera en la comunicación de los seres humanos, ya que la televisión, el chat y los mensajes por celular están reemplazando la interacción directa entre las personas.

El Derecho, como manifestación cultural y rectora de la vida del hombre por excelencia, no está ni puede estar apartada de los incipientes cambios que la ciencia y la tecnología producen en la vida social, sin embargo, los encargados de producción legislativa y los operadores judiciales en general, se han quedado cortos

en cuanto al aprovechamiento de las ventajas tecnológicas en pro del ciudadano. (Iuris Tantum Revista Boliviana de Derecho, 2016)

A partir del uso común de los sistemas informáticos, especialmente con la utilización de las redes sociales, empezaron a aparecer disputas jurídicas que no podían decantarse en soluciones de carácter clásico que presentan dificultades como el carácter jurídico que de los hechos que suceden en internet, la determinación del sitio en que ocurren, para establecer qué tipo de ley aplicar o ante que autoridad judicial acudir y del tiempo en que ocurran los hechos.

Y es en este punto donde la tecnología y el derecho cruzan sus caminos, pues con la dinámica innovadora de la globalización y la Tecnología, han aparecido en todas las ramas del derecho “nuevos” problemas como en temas de responsabilidad civil (responsabilidad de administradores de redes y programadores, en el ámbito del derecho constitucional, al momento de tratar temas como la protección de la intimidad y el derecho a la información, y claramente en los campos del derecho penal cuando se habla de violación a la correspondencia, en este caso de correos electrónicos, la intromisión de los “hackers” y las injurias y amenazas lanzadas en la red bajo el manto del anonimato.

Por lo tanto, la mayor barrera para el desarrollo del Derecho Informático radica en que los sistemas jurídicos actuales en general, no han podido entender la nueva realidad social que nos presenta el mundo actual pues no se ha logrado visualizar a profundidad los cambios que arribaron con el surgimiento de las tecnologías de la información, y aunque se han presentado iniciativas buscando modificaciones, estas han resultado en muchos casos infructuosas, parciales y sin introducir metodologías claras, quedando como solución más próxima a estos dilemas, la introducción de reformas integrales que afecten los ordenamientos jurídicos, y así el derecho pueda absorber este nuevo paradigma tecnológico-comunicacional. (Peña, 2016).

El encuentro de la nueva construcción mental se puede observar en esta imagen:

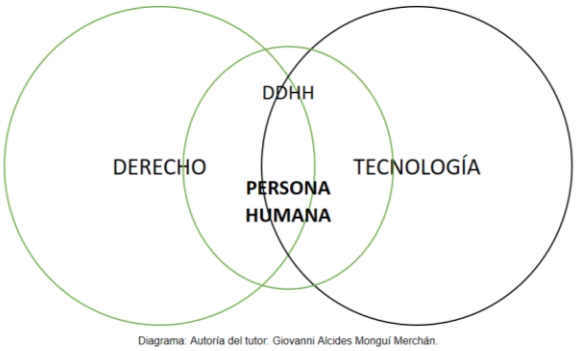

Diagrama: Autoría del tutor: Giovanni Alcides Monguí Merchán.

Nótese entonces, que la relación del derecho y la tecnología es una conjunción y es una intervención del uno y de la otra en sus diversos espectros, ya que, a simple luz, se puede observar sin entrar en minucias como se conjugan, pero al mismo tiempo se yuxtaponen y se traslapan conforme a las circunstancias propias del hecho o de la razón que en todo caso se organiza para la regulación de la conducta y los comportamientos humanos respecto de la utilización de la tecnología.

La conjunción entre derecho y tecnología encuentra su unicidad en la relevancia sistémica que permite que el conocimiento, como ramas del saber no se separen sino que encuentren en sí mismo la correlativa correspondencia epistémica que aporta a las mismas teorías soluciones conceptuales de casos o situaciones que se presentan a diario; pero además de ello como ciencias y técnica no deben separarse en tanto que pragmáticamente se encuentran no solo en la virtualidad sino en la realidad máxime si se trata de la protección de derechos humanos y fundamentales y la persona humana en todo su contexto.

1.2. Relación entre el Derecho Penal y las Nuevas Tecnologías de la Información.

Las innovaciones tecnológicas y sobre todo de las redes informáticas y de comunicación mundial, han dado auge a una nueva Revolución Industrial, cuya base

se sustenta en la información y en cómo esta puede ser almacenada, compartida, de forma ilimitada en cuanto al tiempo y distancia. (Schwab, 2016)

Estos avances no solo beneficiaron a las personas como un método idóneo para acortar distancias, realizando todo tipo de transacciones alrededor del mundo, pues los criminales que antes actuaban atacando directamente a sus víctimas, ahora lo podrían hacer sin tener algún tipo de contacto con estos, y sin que estos supieran quien le causó algún tipo de perjuicio. (Posada Maya, 2017)

De esta manera el derecho tuvo que amoldarse, no solo para proteger la información y los dispositivos, sino para el seguimiento de procesos jurídicos administrativos, de ahí que surgiera la informática jurídica, donde la tecnología es puesta al servicio del derecho. (Posada Maya, Los cibercrímenes: un nuevo paradigma de criminalidad: un estudio del Título VII bis del Código Penal Colombiano., 2017)

Dentro de ese campo se encuentra un área relacionada con el Derecho Penal, la cual consiste en el estudio de delitos donde la informática cumple un papel preponderante como medio para la comisión de ilícitos, los cuales se entienden como delitos informáticos, delitos de alta tecnología o delitos cibernéticos, etc., con lo que el Derecho Penal debió afrontar una nueva forma en que se abordan los conocimientos que desarrollan la conducta punible y sus consecuencias jurídicas, todo en lo que ya habíamos explicado como la sociedad del riesgo. (Sain, 2013)

Entre tanto, el profesor Ricardo Posada Maya, indica que las formas en que el derecho Penal debe cambiar, empiezan en primer lugar desde el ámbito sustantivo, implementando el concepto de conexión y la ejecución virtual de ciberdelitos, lo que implica modificar la importancia y el papel que cumple el nexo de causalidad ontológico-normativo en la teoría del delito, entendido este como la relación de pertenencia que existe entre el comportamiento comisivo y el resultado jurídico ya sea de lesión o peligro, causado por el autor, y en segundo lugar en el ámbito procesal, en cuanto las nuevas Tecnologías de la información y la comunicación, hicieron que las reglas de aplicación del principio de competencia por territorialidad de la ley penal cambiaran, de acuerdo al carácter transfronterizo de los

cibercrímenes, como ocurre también con el fuero del juez para conocer los delitos que ocurren en la web. (Posada Maya, 2017)

Afirma así mismo posada Maya, que es importante analizar también el ámbito punitivo, porque la informática ahora influye de manera determinante en la aplicación de las penas, pues si bien la pena de prisión se erige como la sanción más grave en el ideal que el derecho penal puede imponer, el legislador podría incorporar sancionas alternativas en penas que priven de otros derechos como lo es la inhabilitación para el ejercicio de derechos y funciones informáticas.

Esas restricciones a derechos fundamentales podrían traer consecuencias punitivas mucho más eficaces ya sea como penas accesorias o principales, ya que los efectos son más graves y preponderantes que las penas clásicas de prisión, en términos preventivos, observándolo desde el punto de vista de la víctima y la comunidad, sobre todo en delitos de alta o mediana seguridad como ciberespionaje, ciberlavado, ciberterrorismo, ciberamenazas, delitos sexuales, defraudaciones económicas, delitos contra el orden económico y social, delitos de falsedad informática, etc.

Un ejemplo de lo anterior seria el impacto que podría generar en un individuo la decisión de ser inhabilitado para hacer uso por diez o más años para ser usuario de internet o para adquirir teléfonos celulares con planes ilimitados de datos o el no poder usar determinadas aplicaciones de comunicaciones, etc., buscando con estas determinaciones diseñar mecanismos que permitan hacer eficaces este nuevo tipo de penas, claro está con la colaboración de los prestadores de servicios informáticos o de telecomunicaciones. (Posada Maya, 2017)

En cuanto las características que sobresalen en la relación Derecho Penal - tecnología, (Sain, Derecho y nuevas tecnologías, 2013) detalla que los delitos cometidos en el entorno tecnológico o en el que intervienen dispositivos tecnológicos, ya sean como blanco o fin para el punible, tienen como especialidad frente a otros delitos, en primer lugar a la Transnacionalidad, por la posibilidad que existe de ser realizado desde cualquier parte del mundo usando la red de internet, en segundo término, las dificultades probatorias, esto porque las evidencias digitales y los rastros del crimen son volátiles, otra característica es la

atemporalidad, entendiéndola como la posibilidad de que su ejecución sea programada en determinado día, fecha y hora, como sucede con los virus, otra es que sin duda ha sido una gran barrera en el desarrollo legal del cibercrimen es el anonimato, que permite la construcción de perfiles o identidades falsas en la red y también la inadecuación legal de determinadas conductas ilícitas a las normas penales vigentes, dejando una sensación de impunidad, esto porque el cambio de identidad natural por el de la digital hace más fácil la comisión de delitos como el terrorismo, la pornografía o la pedofilia y las defraudaciones económicas que las personas no harían en un entorno directo o personal, adicionalmente por lo general muchas de estas conductas se realizan en espacios públicos como cafés internet o negocios remotos que carecen de regulación estatal.[4]

Explica así mismo (Sain, Derecho y nuevas tecnologías, 2013), que el delito informático tiene una "cifra oculta" , es decir, que salvo contadas excepciones, estas conductas por lo general no llegan a la Justicia y por lo tanto no hay identificación de responsables y que esto se da porque la velocidad y complejidad de las Tecnologías de la Información y las Comunicaciones, hacen dificultosa su manejo, principalmente por los investigadores que no poseen la pericia necesaria para investigar el punible, y por último, un factor preponderante es el desconocimiento en la gran mayoría de víctimas de delitos informáticos.

II. CONFIGURACIÓN TÍPICA DE LOS DELITOS INFORMÁTICOS EN EL ORDENAMIENTO JURÍDICO COLOMBIANO.

El desarrollo y primeros vestigios de lo que hoy se conoce como delitos informáticos, tiene como punto de partida en los años sesenta cuando por la literatura de esa

[4] Justamente, ABUSO, Derecho penal cibernético. p. 31; BRENNER. Cybercrime and the Law. p. 13; GHDSH/ TURRINI, Cybercrimes: A Multitlisriplinary Analysis, pp. 19 y 20; MIRÓ LLINARES, El eibercrimen: Fenonienología y criminologia de la delincuencia en el ciberespacio. p. 157; SARZANA, Informática, ¡meme! e dirillo penale, pp. 379 y ss.; PICA, Dirilmpenale delle tecnologie lnfor/míliche, pp. 277: UlT, en El ciberdelito. p. 143. señala que "Una de las razones más importantes del 'éxitu' de las páginas web que contienen pornografía incluida la infantil, es que el usuario de internet se siente menos observado desde su casa mientras descarga material de internet"; icl, Understanding Cybercrime, p, 80.
Posada Maya, R. (2017). Los cibercrímenes: un nuevo paradigma de criminalidad: un estudio del Título VII bis del Código Penal Colombiano. Bogotá, D.C. Colombia, Universidad de los Andes. page=58.

época, relacionada con la recolección y almacenamiento de los datos personales en computadoras, se generó un temor general en la población norteamericana, ya que se tomaba como referencia una obra literaria en la que el tema era el de un ser omnipresente que controlaba y vigilaba la vida de las personas usando la tecnología, sumado a que en varios artículos periodísticos de aquel entonces se empezó a hablar por primera vez de delitos informáticos o delincuencia relacionada con computadoras. (Saín, 2015)

Posteriormente, ya en la década de los setenta, empiezan a señalarse casos en lo que hay grandes pérdidas de dinero para empresas del sector privado, los objetivos del delito eran los programas de computación, los datos de investigación en el área de defensa, la información con contable de las empresas y la cartera de direcciones de clientes corporativos. (Saín, 2015)

En los ochenta, los delitos informáticos adquieren una mayor relevancia, a partir de un aumento de fraudes en los que se manipulaba el uso de las tarjetas de débito en cajeros automáticos, vulnerando de las bandas magnéticas, lo que llevó a distintos bancos adoptar la instalación de chips en las tarjetas como medida de seguridad, con lo que se empieza a buscar la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, por lo que la protección legal de las bases de datos de las entidades bancarias se torna algo fundamental para realzar distintas transacciones y negocios, que estuvieran blindados contra el robo de información comercial. (Saín, 2015)

En los finales de los ochenta, empezaron a erigirse los contenidos ilícitos y nocivos en la redes, como amenazas, incitaciones al odio y el intercambio de pornografía infantil y actos de racismo por parte de grupos extremistas, sumado a las técnicas donde se manipulaban sistemas de vuelo y hospitalarios, situación que aumentó a la par con el incremento de usuarios de la red, pasando a ámbitos gubernamentales en 1989, cuando la Justicia de Alemania encontró a hackers que usaban las redes de datos internacionales para el acceso de información reservada de Estados Unidos y Gran Bretaña, con el fin de comercializarla a la KGB. (Saín, 2015)

Ya en los 90s con el incesante crecimiento y apertura exponencial del Internet en Estados Unidos, y la intromisión de las grandes empresas multinacionales en el mundo del comercio electrónico, el dilema se centró en buscar mecanismos que hicieran seguras las operaciones financieras y la compraventa de productos en línea, de igual forma la industria cinematográfica y discográfica, empezó a sufrir casos de violaciones a los derechos de autor con la descarga ilegal de música y películas bajo leyes de copyright, llegando hasta el punto que actualidad conocemos de casos de pedofilia y acosos a los menores en la red, y la intimidad personal que se ve expuesta con el manejo de las tecnologías de la información. (Saín, 2015)

En cuanto al desarrollo jurídico concreto que han tenido distinto países entorno al delito informático, Estados Unidos en 1974, brindo protección a los datos personales en su legislación mediante la “Privacy Act”, que está vinculada con la protección al derecho a la propiedad, enmarcado dentro del contexto del software, pues muchos estados del país norteamericano tipificaron el delito de apropiación ilegitima de programas de computación.

Diez años más tarde se promulgaron las Actas sobre Delitos Informáticos, que tuvieron sus respectivos ajustes en 1986, pero ya en 1994 fueron relegados tras el nacimiento del Acta Federal de Abuso Computacional, herramienta jurídica que trajo consigo figuras delictivas dentro de las que destacan:

- El ingreso a computadoras y sistemas informáticos de carácter federal, contraladas por el gobierno, con la intención de defraudar.
- La adulteración, destrucción o engaño de las claves de seguridad de un sistema informático para boicotear su normal funcionamiento.
- La infección de programas o bases de datos con la finalidad de modificar, copiar o cambiar la operación de las computadoras y redes informáticas.
- Actividades maliciosas que produzcan perdidas económicas a una o varias personas rebasando un monto particular de dinero.

Por su parte El Reino Unido, en 1990 promulgó la “Computer Misue Act” o Ley de Abusos Informáticos, que impone penas de hasta 5 años de prisión o multa, cuando existan alteraciones a los datos informáticos o realizarlos en grado de tentativa.

En Alemania en 1970 se crea por medio de una ley federal un funcionario que es el encargado de la protección de la información cuyas funciones se encaminan a brindar informes periódicos al parlamento sobre cómo funcionan los equipos informáticos públicos, por lo que esta norma fue el antecedente preponderante para que años posteriores se dictará una nueva ley con un alcance más amplio, en el sentido que se protegen los datos de carácter personal contra los abusos del registro, transmisión, modificación y cancelación en el procesamiento de las informaciones.

De igual manera, en 1986 el país germano expidió la Segunda Ley contra la criminalidad económica en la que se plasman algunos delitos informáticos como espionaje, sabotaje, estafa informática, destrucción o daño a un sistema de datos, etc.

En España, si bien en el art. 248 del Código Penal Español de 1995 se encuentra tipificada la conducta de estafa electrónica con ánimo de lucro valiéndose de alguna manipulación informática, esta no está acompañada de alguna sanción o pena privativa de la libertad en caso de su comisión.

En el ámbito latinoamericano, encontramos a Chile, quien fue el primer país de este lado del mundo en sancionar una ley que combatiera los delitos informáticos, en 1993, cuyo contenido se basó en el de la legislación Norteamericana, aunque su eje central versa sobre el apoderamiento, uso o conocimiento indebido de la información contenida en un sistema informático con el fin de revelarla y/o difundirla. (alfa-redi.org, 2015)

2.1. Conceptualización del delito informático

Para tratar de adentrarnos en el estudio concepto general de delito informático es importante conocer algunas de las significaciones hechas por varios juristas y doctrinantes.

La primera que encontramos es la que definen Mario Arboleda Vallejo y Jose Ruiz Salazar, refiriendo a los delitos informáticos como un comportamiento ilegal o contrario a la ética o no autorizado que conlleva un tratamiento automático de datos y / o una transmisión de datos. (Arboleda Vallejo & Ruiz Salazar, 2017)

Por su parte Téllez Valdés determina a los delitos informáticos según dos elementos fundantes, el primero cuando se usa el computador como instrumento o medio, es decir que el delincuente se vale de la computadora "*como método, o símbolo en la comisión del ilícito"*, el segundo cuando el computador se usa como como fin u objeto, las conductas delictivas se dirigen directamente contra el aparato, sus accesorios y programas. (Téllez, 1997)

Entre tanto Pérez Luño, realiza una clasificación, desde el punto de vista subjetivo, objetivo y funcional. En el subjetivo, plantea el estudio del delincuente y a sus características, por ejemplo, si se trata de delitos de cuello blanco, relaciones de poder frente al sistema o simplemente si es una persona del común. En el aspecto objetivo, señala el autor, que se examinan los daños que las conductas delictivas causaron, delimitando al delito y su "modus operandi", así: a) Los fraudes (Manipulaciones contra los sistemas de procesamiento de datos), b) (El sabotaje informático (Bombas lógicas, virus informático. C) El espionaje informático y el robo o hurto de software. D) El robo de servicios, e) El acceso no autorizado a servicios informáticos. Y por último está el aspecto funcional, que observa el proceso informático o de datos, y partiendo de este realiza una clasificación de los delitos informáticos así: Delitos contra la fase de entrada del sistema, delitos contra la fase de salida del sistema, atentados contra los programas del sistema y atentados contra la elaboración, procesamiento de datos y comunicación, telemática. (Cuervo Álvarez, 1999).

Por su parte el profesor Ricardo Posada Maya, explica que desde hace años se ha acostumbrado a aplicar las teorías del delito, fundado en imputación objetiva y subjetivo al autor de conductas que producen un cambio un cambio o alteración en el mundo exterior, como los homicidios, hurtos, incendios, etc., sin embargo con la aparición de los delitos informáticos en los años setenta, se ha abierto el camino

para replantear las nociones y categorías dogmáticas usadas normalmente en el ámbito punitivo para resolver las responsabilidades, esto porque los punibles cibernéticos se enmarcan dentro de una nueva especie de campo de acción, donde la virtualidad y el uso de los medios tecnológicos han irrumpido tanto de manera positiva o de manera negativa, delitos que tienen su incidencia en un lugar o ámbito deslocalizado como lo es la web y el ciberespacio, situaciones que generan interrogantes y dan pie para que exista una transformación sustantiva sobre la pena y el delito, en el entorno tecnológico. (Posada Maya, 2017)

Observadas las anteriores concepciones se podría definir a los delitos informáticos como actos o comportamientos, que cumplen con la adecuación típica, y que resultan gravosas a derechos o intereses de personas ya sea naturales o jurídicas, desarrolladas bajo el escenario del ciberespacio e internet, y que usan generalmente como medio el computador, otros aparatos tecnológicos y demás componentes.

2.2. Características del delito informático

Sobre las particularidades diferenciales de esta clase de delitos, el jurista Mexicano Julio (Tellez Valdéz, 2005) determina una serie de elementos preponderantes en el que se destacan las siguientes:

a). En primer lugar, se expresa que son conductas criminales de cuello blanco o *White collar crime,* ya que un número reducido de personas, que posean ciertos conocimientos técnicos, pueden llegar a cometerlos de manera concreta.

b). Otra distinción de este tipo de delitos radica en que este tipo de acciones son de tipo ocupacional, en el entendido que en la mayoría de los casos se materializan cuando el sujeto activo se encuentra trabajado.

c). Son acciones de oportunidad, ya que se aprovecha una ocasión creada en el mundo casi infinito de funciones y organizaciones del sistema tecnológico y económico.

d). Provocan un perjuicio económico, ya que, en muchas ocasiones, el delincuente apunta hacia el patrimonio que posee el sujeto pasivo.

e). Ofrecen posibilidades en cuanto a tiempo y espacio, pues en cuestión de milésimas de segundo y sin necesidad de la presencia física, puede llegar a consumarse el punible.

f). Existe una característica que destaca por la verdad que revela y es la referente al sinnúmero de casos que ocurren a diario, pero que no son denunciados por las víctimas, ya sea por desconocimiento o falta de regulación normativa en algunos casos.

g). Son muy sofisticados y muy asiduos dentro de los temas estratégico-militares.

h). Poseen un gran defecto probatorio, al ser complicada su comprobación, precisamente por el tecnicismo que manejan y por el rastro dejado en la web que muchas veces es difícil de recuperar.

i). En algunos casos, su consumación resulta imprudencial o accidental, es decir, que no hay un fin determinado a causar daño. (Tellez Valdéz, 2005).

j). Es una manifestación delictual de acto y no de mera conducta, ya que necesitan de una modificación lógica o informática sobre el objeto sobre el cual recae la acción criminal, y que de todas maneras no siempre se manifiesta con una alteración en el mundo exterior físico, ya que al hablar de los delitos informáticos estamos sujetos a un nuevo paradigma en el que se debe observar un daño o alteración inmaterial del objeto que en este caso son los datos informáticos interceptados, cuya tangibilidad no es de fácil determinación.

Podría concluirse de lo anterior, que el delito informático tiene unas particularidades únicas que le son propias del sujeto activo, el cual requiere una cualificación que le es propia para ejecutarlo, ya sea de forma dolosa o culposa. Que en su determinación incurre una apropiación de conocimientos técnicos para llevar a cabo determinado comportamiento que causa daños en las relaciones de las personas y la tecnología, afectándose con esto su persona, su patrimonio e intereses, figuras inherentes a una persona natural o jurídica, atacando entre otros, la confiablidad,

confidencialidad, integridad, disponibilidad, habeas data, es decir el derecho a la libre disposición, inviolabilidad, almacenamiento y transmisión de datos e información digital, etc.

Los anteriores rasgos distintivos decantarían en un tratamiento especial de los delitos informáticos, ya que se trata de comportamientos en los que se utiliza como medio y fin las tecnologías de la información y los datos informáticos, lo que requiere de plano unos conocimientos técnicos y profesionales por parte del personal investigativo y judicial para que la persecución y juzgamiento de estos ilícitos no se vea truncado por imprecisiones o errores en la apreciación y recolección de los elementos materiales probatorios y evidencias recaudadas durante las distintas etapas del proceso penal o en el manejo de terminología; adicionalmente, el sujeto activo protagonista en este campo jurídico informático en la mayoría de casos es el llamado delincuente de cuello blanco, cuya identificación concreta se torna compleja al estar estos individuos ligados a empresas o redes transnacionales dedicadas a cometer delitos informáticos de manera global, escenario que requiere de una articulación estructurada de los órganos de policía en la gran mayoría de países con el fin de facilitar la ubicación de los delincuentes informáticos y sobre todo el de judicializar penalmente a las personas jurídicas de derecho privado, figura que desafortunadamente no encuentra actualmente regulada en nuestro país.

2.3. Surgimiento del delito informático en el ordenamiento jurídico colombiano.

Esta modalidad delictiva tiene su génesis en el ordenamiento Jurídico Colombiano el 5 de enero de 2009, cuando el (Congreso de la República de Colombia, 2009) promulgó la Ley 1273 de 2009, “Por medio del cual se modifica el Código Penal, y se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”,

la cual estuvo cimentada en los lineamientos establecidos en el (Convenio de Budapest del Consejo de Europa contra la cibercriminalidad., 2001)

Este convenio fue suscrito el 23 de noviembre de 2001 y entro en vigor el 1 de julio de 2004 en Budapest, Hungría, tratado internacional que tenía como fin la protección a la sociedad frente los delitos informáticos y delitos en internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y por su puesto la Cooperación internacional de los países que ratificaron el convenio.

Este convenio consiste en el único acuerdo internacional sobre delitos informáticos que fundamentalmente hace énfasis en las infracciones de derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. Gracias al reconocimiento de la necesidad de prevenir dichos actos que puedan poner en peligro la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, es que se determina la lucha eficaz contra estos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo acciones que permitan una cooperación internacional rápida y fiable, de igual forma busca unificar las definiciones sobre ciberdelito, establecer el intercambio de información en lo que respecta a estos ilícitos, garantizar el debido equilibrio entre los intereses de la acción penal y el respeto a los derechos humanos que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada. (NIC Argentina - Dirección Nacional del Registro de Dominios de Internet,, 2017)

Colombia, con la expedición de la Ley 1928 del 24 de julio de 2018, aprueba y se adhiere formalmente al Convenio sobre cibercriminalidad de Budapest, representando esta norma un importante instrumento jurídico para el país, ya que facilita el avance con acciones decididas contra la criminalidad en internet en el ámbito internacional.

Con la promulgación de la ley 1273 de 2009, el delito informático se enfocó primordialmente en la protección de la información y los datos, estructurando su

contenido en dos apartados: Por una parte, se encuentran las conductas lesivas contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. (Código Penal, arts. 269A y s.s.) En segundo término, están los delitos informáticos, que se circunscriben al hurto de medios informáticos y la transferencia no consentida de activos. (arts. 269I Y 269J).

El legislador con la implementación de este articulado, buscaba que Colombia se pusiera a la par de los países miembros de la Comunidad Económica Europea, quienes pretendieron extender internacionalmente acuerdos jurídicos que estuvieran relacionados con la protección de la información y los recursos informáticos de los países, como lo es el ya mencionado Convenio contra la cibercriminalidad de Budapest, Hungría, en el 2001.

En síntesis, La ley 1273 de 2009 es la expresión jurídica de la evolución social de un mundo que actualmente está interconectado por las redes de la internet, y de la intervención de la tecnología en las conductas humanas y de derecho, así como de la intervención del derecho en la tecnología, que desde los años ochenta empezó a disminuir las barreras nacionales, para dar paso un universo virtual, en el que usuarios, datos y sistemas, a pesar de existir grandes distancias entre uno y otro lugar y no encontrarse presencialmente, se enmarcan dentro de un mismo entorno o mundo tecnológico.

En lo que respecta al contenido de la Ley, en su artículo 1° se adiciona y actualiza el Código Penal a las regularidades comportamentales del mundo globalizado, para poder criminalizar y perseguir penalmente, tanto en el ámbito nacional como internacional.

En lo que respecta a los tipos penales, en primer lugar se encuentra el artículo 269A el que describe el acceso abusivo a un sistema informático, delito que se configura cuando el sujeto activo, como puede ser un hacker, aprovecha las pocas barreras (cortafuegos) que por lo general tienen los sistemas de información en los procedimientos de seguridad de las organizaciones, con el fin de extraer información que genere réditos económicos o que ponga de presente la paupérrima capacidad

de los mecanismos y recursos tecnológicos. (Manjarrés & Jímenez, 2012) (Congreso de la República de Colombia, 2009)

En el artículo 269B se contempla el delito de la “obstaculización ilegitima del sistema informático o red de telecomunicación”, que tiene su origen cuando el sujeto activo bloquea en forma ilegal determinado sistema o niega su ingreso por un tiempo, que resulta suficiente para obtener un provecho generalmente de tipo económico. (Manjarrés & Jímenez, 2012) (Congreso de la República de Colombia, 2009)

El artículo 269C, refiere la conducta relacionada con “la interceptación ilícita de datos informáticos”, que se exterioriza cuando una persona, haciendo uso de los elementos tecnológicos necesarios, obstruye datos ya sea en su origen, en el destino o en el interior del sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los transporte, todo esto sin la respectiva autorización Judicial. (Manjarrés & Jímenez, 2012). (Congreso de la República de Colombia, 2009)

El artículo 269D, explica lo referente al delito de “daños informáticos” y que se presenta cuando el sujeto activo sin estar autorizado, modifica, altera, daña, borra, destruye o suprime datos de un programa o de documentos electrónicos, en los recursos de las TIC. (Manjarrés & Jímenez, 2012) (Congreso de la República de Colombia, 2009)

El artículo 269F estipula el delito de “uso de software malicioso” o también llamado “malware” en el mundo de la internet, cuya comisión se da cuando se producen, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que buscan producir daños en sistema informático determinado. (Manjarrés & Jímenez, 2012) (Congreso de la República de Colombia, 2009)

En el artículo 269F, se encuentra plasmado el delito de “violación de datos personales”, referente al actuar de una persona que sin estar facultado sustrae, vende, envía, compra, divulga o emplea datos personales guardados en ficheros, archivos, bases de datos o medios parecidos, con el fin de obtener provecho para

sí o para terceros; punible que está orientado a proteger los derechos fundamentales a la dignidad humana y libertad de expresión. (Manjarrés & Jímenez, 2012) (Congreso de la República de Colombia, 2009)

El artículo 269G habla de la “suplantación de sitios web para capturar datos personales”, que se materializa cuando el delincuente suplantador o “pisher” crea una página web y un dominio con una fachada similar al de la entidad a la cual se desea suplantar, ubicando dicha página en un determinado servidor, desde donde envía correos spam o basura engañosos, como ofertas de empleo o premios, situación que hace difícil distinguir la página original de la falsa, incurriendo en el error a las personas que sin saberlo otorgan información personal y claves bancarias que el suplantador guarda en una base de datos ordenando posteriormente la transferencia del dinero de la víctima a cuantas de terceros, que prestan sus cuentas, para que luego sean reclamadas o distribuidas. (Manjarrés & Jímenez, 2012) (Congreso de la República de Colombia, 2009)

En lo que respecta a las Circunstancias de agravación punitiva, se encuentran descritas en el artículo 269H, y entran en escena cuando el delito se comete en redes, sistemas informáticos y de comunicaciones pertenecientes al Estado, al sector financiero nacional o extranjero; o cuando se origine o promueve por un funcionario público; o cuando se da a conocer información confidencial en perjuicio de otro para obtener provecho propio o de terceros; también cuando se actúa con fines terroristas para atentar contra la seguridad o defensa nacional; o cuando se usa como instrumento a un tercero de buena fe. (Congreso de la República de Colombia, 2009)

Colofón a lo anterior, si quien comete las conductas descritas, es el responsable de la administración, manejo o control de la información susceptible de delito, se le impondrá además hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales. (Manjarrés & Jímenez, 2012) (Congreso de la República de Colombia, 2009)

De igual manera es importante anotar que la Ley 1273 de 2009, añade como circunstancia de mayor punibilidad en el artículo 58 del Código Penal, realizar conductas utilizando medios informáticos, electrónicos o telemáticos**.** (Manjarrés & Jímenez, 2012)**.**

2.4. El Caso de Andrés Fernando Sepúlveda Alias "El Hacker".

A pesar de la significativa influencia que las nuevas tecnologías de la información ha tenido en los diferentes aspectos de la vida económica y social de las personas, sumado a la legislación que entró a regir en nuestro país desde el 2009, han sido pocos los casos que han asomado la cabeza en el universo jurídico Colombiano, situación que no debería ser algo que llame la atención, pues los delitos informáticos son relativamente novedosos respecto a los clásicos delitos que conocemos, sin embargo a continuación se referencia un caso de gran relevancia nacional, sobre todo por las implicaciones políticas que trajo consigo, principalmente a la hora de plantear nuevas estrategias que faciliten el acercamiento con los votantes, tal como ocurrió en el año 2014 en épocas de elecciones presidenciales en nuestro país, cuando causó gran revuelo la captura de Andrés Sepúlveda, conocido como el "hacker", a quien se le acusó de pertenecer y comandar una oficina en la que se realizaban interceptaciones ilegales, hechos que se apuntaron con elementos materiales probatorios allegados a la Fiscalía, que permitieron acusar a Sepúlveda de "monitorear ilegalmente el proceso de negociación de la habana, a través de correos y extracción de documentación por medio de técnicas de HACKIN, en una oficina de la ciudad de Bogotá" (Fiscalía General de la Nación, 2014)

A raíz de esto, el 10 de abril de 2015, el Juzgado 22 penal del Circuito de Bogotá, sentenció a Sepúlveda a través de un preacuerdo, a 10 años de prisión por los delitos de Espionaje, Concierto para delinquir agravado, ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO, USO DE SOFTWARE MALICIOSO Y VIOLACIÓN DE DATOS PERSONALES AGRAVADO, erigiéndose esta resolución judicial como la primera condena por espionaje en la historia de Colombia. (Fiscalía General de la Nación, 2014).

La Jueza en dicha providencia determinó que con los Elementos Materiales Probatorios allegados por la Fiscalía, se demostró la existencia de las conductas punibles imputadas y aceptadas en virtud del preacuerdo por parte de Sepúlveda, en las que se observó la intención dolosa de vulnerar la Seguridad Pública, la Protección de la Información y de los datos y la Seguridad del Estado, ya que se probó que durante el mes de enero y mayo de 2014, Sepúlveda y Otras personas se concertaron bajo la organización y dirección del primero, con el fin de cometer delitos con permanencia en el tiempo, actividades ilícitas que se materializaban en varios inmuebles de la ciudad de Bogotá, configurándose además la circunstancia de agravación punitiva establecida en el inc. 3° ya que Sepúlveda fue quien organizó, fomentó, dirigió y financió la comisión de delitos informáticos. (Sentencia Condenatoria contra Andres Fernando Sepúlveda , 2015)

De igual manera se determinó que Sepúlveda, cometió en calidad de coautor, el delito de ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO AGRAVADO, ya que, sin autorización él y otros accedieron al correo electrónico de alias “BORIS”, miembro de la mesa de negociación de la Habana y Jefe de prensa de las FARC, acciones con las cuales se puso en peligro la Seguridad Nacional, Configurándose así, la circunstancia de agravación punitiva consagrada en el artículo 269H numeral 6° del Código Penal. (Sentencia Condenatoria contra Andres Fernando Sepúlveda , 2015)

El otro delito del que se estableció la comisión por parte de Sepúlveda, en calidad de coautor, fue el de VIOLACIÓN DE DATOS PERSONALES AGRAVADO, ya que se probó que él y otro, sin estar facultados y con provecho propio, obtuvieron y compilaron archivos que contenían los perfiles de los negociadores de las FARC en la Habana, archivos que posteriormente fueron divulgados por Sepúlveda en la página por el creada dialogosavoces.@.com, además obtuvo compiló archivos fílmicos en los que se hacen presentaciones de guerrilleros pertenecientes a las FARC, también obtuvieron indebidamente bases de datos de la Policía Nacional, del Ejercito Nacional y de la Agencia Colombiana para la Reintegración, revelando información exclusiva de las agencias de inteligencia y seguridad del Estado,

información clasificada como secreta y ultra secreta, entre los que se encontraban datos personales de los reinsertados desde el año 1993 a 2008, generando con esto un riesgo para la seguridad y defensa nacional, adecuándose de igual forma la agravación punitiva del artículo 269H del Código Penal. (Sentencia Condenatoria contra Andres Fernando Sepúlveda , 2015)

Finalmente se encuentra el delito de USO DE SOFTWARE MALICIOSO, del cual se demostró su comisión por pate de Sepúlveda en calidad de coautor, en la medida que él y otros sin estar facultados para ello, produjeron un software malicioso o “virus”, con el cual se pudo acceder al dominio del sistema informático del ex vicepresidente de la republica Francisco Santos Calderón. (Sentencia Condenatoria contra Andres Fernando Sepúlveda , 2015)

Se destaca el Juicio de reproche esgrimido por el juzgador en el que resalta el aprovechamiento por parte de Sepúlveda, de sus habilidades y destrezas en el manejo de sistemas informáticos para vulnerar el Bien Jurídico con el que el legislador propendió tutelar con la creación de la Ley 1273 de 2009, es decir la información y los datos personales de todos los Colombianos, que si bien podrían tratarse de Derechos de Tercera Generación, estos están asociados a Derechos fundamentales como el de la libertad, el libre desarrollo de la personalidad, la intimidad y hasta el derecho a la propiedad privada.

III. EL TIPO PENAL DE INTERCEPTACIÓN DE DATOS INFORMÁTICOS EN COLOMBIA.

3.1. Aproximación conceptual sobre la Interceptación de datos

Existen varios tipos de amenazas o riesgos que acechan a los sistemas informáticos, ya sea que estas provengan de conductas humanas, softwares maliciosos o desastres de la naturaleza

Precisamente una de esas variedades de riesgos que se manifiestan en los sistemas informáticos es el de la interceptación, el cual se determina cuando el atacante accede a la información que se ha enviado, pero esta también llega al destino original; este caso, es conocido en el argot de la informática como el de los “sniffers” informáticos.

Este acto interceptación atenta directamente contra el principio de confidencialidad del que deben gozar los datos e información de los sistemas informáticos.

La confidencialidad o también denominada como “secreto”, es un criterio el cual se encamina a que la información únicamente esté disponible para aquellas personas o “usuarios” que tengan la respectiva autorización para hacerlo. (Maillo Fernández, 2018)

De igual manera es menester tener claro las diferencias del acto de interceptación con otras acciones que atentan contra los sistemas informáticos y la información que contienen.

En primer lugar se encuentra la *interrupción*, en la que se impide que la información llegue desde el origen al destino, que puede manifestarse con la destrucción de algún dispositivo de red o con el robo de la información durante su trayecto; acción que arremete contra el principio de disponibilidad de la información. (Maillo Fernández, 2018)

Otra amenaza es la *Modificación,* que se presenta cuando un atacante accede a la información enviada, la cambia y se la hace llegar al destino una vez modificada, haciéndole creer que fue remitida inicialmente de esa manera; acción que atenta contra el principio de integridad de la información. (Maillo Fernández, 2018)

Por último se encuentra la *Fabricación*, que se manifiesta cuando el atacante no intercepta ninguna información, si no que crea una propia y la envía al destino haciéndose pasar por el origen que quiera suplantar, amenaza que atenta contra el principio de integridad (Maillo Fernández, 2018)

Es así, que nace como protagonista idóneo para combatir la interceptación, el tipo penal regulado en el Código Penal Colombiano en el artículo 269C y ubicado en el

Titulo VII BIS que habla De La Protección de la información y de los datos, bien jurídico tutelado que se creó con la expedición de La ley 1273 del 5 de enero de 2009.

Dicho tipo penal preceptúa lo siguiente:

"ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses. (Congreso de la República de Colombia, 2009)

Esta conducta punible consiste en el hecho de interceptar datos informáticos de carácter personal, ya sean privados o semiprivados de naturaleza económica, o de carácter impersonal, bien sea en el sistema informático donde provienen (origen), durante su transmisión NO pública por canales físicos o inalámbricos como por ejemplo el WI–FI, o también en el sistema informático a donde son enviados, es decir el destino al que hace referencia el tipo penal.

En ese entendido, se incurre en el tipo penal sin importar que el sujeto activo intercepte los datos en el medio, los altere o modifique, para enviarlos nuevamente al sujeto de destino, caso en el cual entra en acción otro delito, referente a los daños informáticos, en la modalidad de alteración (art.269D). (Posada Maya, 2017)

Lo autores Mario Arboleda Vallejo y José Armando Ruiz Salazar indican que el fin del delito es sancionar la interceptación ilícita de datos informáticos, teniendo claro que dicha ilicitud no versa sobre razones de fondo, si no tiene que ver con el requisito explicito que trae el tipo penal: la orden judicial previa.

Indican de igual manera estos autores que la interceptación de los datos se puede realizar utilizando medios telemáticos como el internet, donde para obtener la información deseada se capturan las modulaciones generadas por el computador o el sistema informático objeto de interceptación, y posteriormente se desmodulan

través de un modem, obteniendo así el contenido de la información o datos que recorren el cableado. (Arboleda Vallejo & Ruiz Salazar, 2017)

El artículo tercero del Convenio del Consejo de Europa sobre la Ciberdelincuencia, se pronuncia sobre la interceptación ilícita, refiriendo que el Estado parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá· exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático. (Convenio de Budapest del Consejo de Europa contra la cibercriminalidad., 2001)

En el Código Penal Español existe un artículo que guarda similitudes con el tipo penal descrito en nuestra legislación y es el 197.1, igualmente reformado por la ley orgánica No. 5 de 2010, que describe lo siguiente: El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. (Escobar & Jimenez, 2018)

En la norma antes referenciada se detallan como sanción tanto la multa como una pena privativa de la libertad, lo cual se diferencia de lo que determina la legislación colombiana, ya que en esta última se establece una pena de prisión “De treinta y seis (36) a setenta y dos (72) meses” sin que haya una sanción de carácter pecuniario.

3.2. Descripción del tipo penal de interceptación de datos en Colombia

En cuanto al análisis estructural del delito, autores como Jorge Martínez Valencia refieren que el tipo penal castiga a quien sin “Previa orden judicial intercepta datos protegidos en su origen, destino o en el interior de un sistema informático, y de igual modo, a quien intercepte las emisiones electromagnéticas de un sistema que las transporte”. (Escobar & Jimenez, 2018)

Explica así mismo, que este tipo penal al igual que los punibles de Acceso Abusivo a sistema informático y obstaculización ilegitima de sistema informático, protege la “Libertad informática, y a más de esto, la protección de la información y los datos reservados encerrados en la expectativa de la esfera privada de la intimidad, valores trascendentes de ámbito personal y social”. (Escobar & Jimenez, 2018)

Por su parte el profesor Ricardo Posada Maya, realiza un análisis del aspecto objetivo del tipo explicándolo de la siguiente manera:

Sujeto activo

En lo que respecta al sujeto activo de la conducta, explica Posada Maya que es de carácter mono subjetivo y común, pues se habla de “El que”, indicando que puede realizarla cualquier persona, permitiendo de igual forma la coautoría y las distintas formas de participación criminal como la determinación y la complicidad.

Un punto clave a tener en cuenta es que si bien estos delitos informáticos son de mayor predominancia en el ámbito de la criminalidad organizada transnacional mientras en nuestro país no se instaure la responsabilidad penal de las personas jurídicas, ya que no es posible apuntar la comisión del delito a una organización en concreto. (Posada Maya, 2017)

Sujeto pasivo

El sujeto pasivo en la interceptación de datos informáticos, puede ser una persona natural o una persona jurídica de derecho público o privado, pero además del titular encargado de la seguridad e integridad de la información de los usuarios, también son sujeto pasivo los titulares de los datos que son violados en los sistemas informáticos interceptados o de las emisiones electromagnéticas que provengan de los sistemas que transportan datos, como por ejemplo las ondas de telefonía celular. (Posada Maya, 2017)

Bien Jurídico

La Interceptación de Datos informáticos, es de carácter pluriofensivo, ya que en primera instancia el tipo penal se establece la lesión no consentida de la seguridad de la información y las funciones informáticas, es decir el tratamiento seguro y confiable de las transmisiones no públicas de datos por medio de sistemas informáticos y redes de comunicaciones.

De igual forma, esta conducta punible atenta no solo contra el bien jurídico de la seguridad de las funciones informáticas (confiablidad, confidencialidad, integridad, disponibilidad, etc.), si no también ataca el habeas data, es decir el derecho a la libre disposición, inviolabilidad, almacenamiento y transmisión de datos e información digital, consagrado en el artículo 15 de la Carta Política. (Posada Maya, 2017)

Objeto sobre el cual recae la acción

Este punible recae en primer lugar, sobre las transmisiones o transferencias no públicas de datos informáticos, en su origen, destino o en el curso de la transmisión informática, teniendo claro que estas maniobras deben ser contra comunicaciones que sean netamente informáticas, pues en caso contrario se incurriría en el punible de violación ilícita de comunicaciones del art. 192 del Código Penal.

Cabe resaltar que cuando se hace referencia a que la interceptación debe recaer sobre transmisiones no públicas de datos personales o impersonales, es claro que son del ámbito punible las transmisiones públicas de datos de naturaleza pública, pues su tratamiento y conocimiento es totalmente ilimitado y sin restricción alguna.

El segundo objeto sobre el cual recae la acción en este delito, son las emisiones electromagnéticas, que son oscilaciones de partículas electromagnéticas y eléctricas producidas por un equipo o dispositivo durante su funcionamiento, y en concreto cuando se transmiten datos, y si bien ese tipo de emisiones no pueden considerarse como datos en sentido estricto, ya que no es información que pueda ser tratada mediante sistemas informáticos, si pueden ser interceptados en el espacio electromagnético, porque se pueden reconstruir datos a partir de dichas emisiones.

En punto de los agravantes que indica artículo 269H, en su numeral 1, advierte la agravación de la pena de interceptación de datos informáticos de la mitad a las tres cuartas partes cuando la acción recaiga sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros, buscando con esta medida proteger los sistemas informáticos, cuando de por medio están inmersos temas político criminales y de convencía social que podrían poner en peligro inminente otros bienes jurídicos conexos. (Posada Maya, 2017)

Verbo Rector

El tipo penal trae dentro de su descripción típica el término “intercepte”, interceptar transmisiones por medios técnicos en con el fin de obtener datos informáticos, comunicaciones o emisiones electromagnéticas sin ningún tipo de consentimiento. Interceptar se podría asemejar a adquirir, ver y capturar comunicaciones de datos informáticos en movimiento, sin que se permita el arribo a su destino, o impidiendo su respectiva transmisión.

Otra de las características que se erigen en la acción de interceptación, enmarcada dentro del delito objeto de análisis, es que su consumación es de carácter instantáneo, en la medida que el sujeto activo materializa de manera inmediata y con una sola acción la interceptación de transmisiones o procesamiento de datos informáticos en el sistema de origen, o el en proceso de transmisión, o del sistema informático de destino de los datos enviados o transmitidos.

Asimismo, la conducta permite dar aplicación a la figura de la tentativa establecida en el art. 27 del C.P., cuando el autor solo puede realizar una manipulación informática, pero no logra interceptar en sentido estricto datos, comunicaciones de datos informáticos o emisiones electromagnéticas.

Otra cualidad que presenta este tipo penal, es que al ser de resultado, permite su realización en la figura de comisión por omisión del art. 25 del C.P., cuando el autor responsable hubiese tenido el deber de garante de no permitir que personas sin la debida autorización intercepten la transmisión de datos en su origen o transmisión, por lo tanto se debe demostrar que a quien se le atribuye la omisión tenía a su cargo la protección específica de un bien jurídico o que se le haya encargado la vigilancia de una fuente de riesgo determinada. (Posada Maya, 2017)

Dolo

Entrando en el aspecto subjetivo de la conducta, para acreditar el dolo es imperioso que el autor conozca indudablemente y quiera realizar ya sea de manera directa, remota o programada, conductas destinadas a interceptar datos informáticos transmitidos mediante comunicaciones no públicas, o las emisiones electromagnéticas que devengan del funcionamiento de estos sistemas.

De igual manera el conocimiento del dolo debe cobijar el querer y la conciencia de que se actúa “sin orden judicial previa” o sin la expresa autorización del titular de las trasmisiones interceptadas, queriendo decir con esto que el autor del punible no tiene la facultad de disponer o acceder a las transmisiones de datos informáticos o emisiones electromagnéticas. (Posada Maya, 2017)

Por último es significativo acotar que el tipo penal no demanda para su materialización que el autor de la interceptación tenga un fin criminal más distante como podría ser el divulgar a terceros los datos interceptados, sin embargo en este caso la conducta se podría agravar, según lo establece el art. 269H núm. 4 por haberse revelado el contenido de la información con el fin de perjudicar a otra persona, lo que implica una mayor afectación pues ya entra en juego el bien jurídico de la intimidad personal. (Posada Maya, 2017)

IV. CONTINGENCIAS EN LA CONFIGURACIÓN Y APLICACIÓN DEL TIPO PENAL DE INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

Como ya se indicó anteriormente, al ser la Interceptación de datos informáticos un tipo penal simple por tener como único verbo rector el de “interceptar” dentro de su estructura típica, sumado al hecho de que esta conducta podría denotarse como de sujeto activo simple, ya que lleva consigo la expresión “el que”, se infiere entonces que no se requiere una característica especial del sujeto que pueda incurrir en el tipo penal, situación que a priori no detentaría ninguna discusión, pero que al analizar con más detenimiento se encuentra que en el delito el sujeto activo debe ser una persona que posea una calidad especial como ser funcionario de Policía Judicial.

Lo anterior aflora en la medida que este funcionario es el encargado de realizar las respectivas investigaciones judiciales a lo largo del desarrollo del proceso penal y que para realizar sus funciones y actividades de manera eficaz, requiere de una orden judicial previa para poder hacer las interceptaciones a datos informáticos según corresponda, tal y como lo pide el tipo penal. (Vasquez Santamaría & Mesa, 2012)

Precisamente la Ley 906 de 2004 expresa el deber que tiene la Fiscalía General de la Nación de informar a la autoridad competente de cualquier irregularidad que advierta en el trasegar de la actuación de los funcionarios que ejerzan las funciones de policía judicial (Art. 142 Núm. 4, L. 906 de 2004). En ese sentido, lo que se puede

inferir de todo lo anterior, es que el sujeto activo en el punible de interceptación de datos informáticos, no puede tratarse de un sujeto cualquiera, si no debe ser una persona que cuente con los conocimientos técnicos suficientes para ejecutar la interceptación. (Vasquez Santamaría & Mesa, 2012)

Po otra parte, la Ley 906 de 2004 señala en el art. 235 las distintas actividades y elementos que pueden ser objeto de investigación, y en las que no es necesario la autorización del Juez de Control de Garantías, entre las que se encuentran la de la actividad de interceptación de comunicaciones que indica lo siguiente:

"*ARTÍCULO 235. INTERCEPTACIÓN DE COMUNICACIONES TELEFÓNICAS Y SIMILARES. [Artículo modificado por el art. 52 de la ley 1453 de 2011. El nuevo texto es el siguiente:] El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación, así como del procesamiento de la misma.* ***Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación.***

En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.

Por ningún motivo se podrán interceptar las comunicaciones del defensor.

La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron.

La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías." (Congreso de la Republica de Colombia).

Al respecto, la Corte Constitucional en Sentencia C-334 del (2010), se pronunció indicando que la interceptación de comunicaciones, requiere de un control judicial

posterior, concepto que no va de la mano con el de la orden judicial previa que describe el tipo penal de interceptación de datos informáticos, manifestando lo siguiente:

"*Con la modificación introducida al artículo 250 constitucional por el Acto Legislativo No. 3 de 2002, se contemplan, en términos generales, tres tipos de intervención por parte de la Fiscalía. Una primera, la habilitación legal para "realizar excepcionalmente capturas", la cual se somete, al tenor del numeral 1º, a un control de legalidad posterior dentro de las 36 horas siguientes a la práctica de la medida; otra, en la cual se contemplan los "registros, allanamientos, incautaciones* ***e interceptaciones de comunicaciones****", que también conforme al inciso 2º,* ***son controlados con posterioridad a su práctica y dentro de las 36 horas siguientes;*** *y finalmente, las demás "medidas adicionales que impliquen afectación de derechos fundamentales", previstas en el numeral 3º, las que sí requieren "autorización por parte del juez que ejerza las funciones de control de garantías para poder proceder a ello", con lo que se quiere significar que, salvo la práctica de exámenes sobre la víctima de delitos o agresiones sexuales, las intervenciones de la Fiscalía que requieren autorización judicial, operan sobre la persona contra quien cursa la investigación."* Negrillas y resaltado fuera de texto.

Por lo tanto se reafirma por parte del máximo órgano Constitucional, el mandato legal del control judicial posterior que debe realizar la Fiscalía cuando ordene realizar la interceptación de comunicaciones en el marco de una investigación procesal penal. (Vasquez Santamaría & Mesa, 2012)

En los mismos términos en la Sentencia C-336 del (2007), la Corte enfatizó el requisito para la interceptación de comunicaciones del control "posterior" como una regla general, buscando así fortalecer dentro del sistema acusatorio de investigación penal el principio de reserva judicial, cuando de la afectación de derechos fundamentales se trate.

Visto lo anterior, se entiende como por vía jurisprudencial se despeja el camino hacia la interpretación que debe dársele a la acción tipificada en el tipo penal del artículo 269C, el cual tendría una doble garantía, siendo la primera la necesidad de

obtener orden judicial previa, obedeciendo los postulados que buscan proteger el derecho a la intimidad, y como segundo precepto, se requiere de la orden judicial posterior que por mandato de la ley, debe realizar el funcionario que cumpla con las funciones de policía Judicial, en el momento de realizar la respectiva interceptación.

V. A MANERA DE CONCLUSIÓN

En la actualidad y con el continuo abordaje que la globalización va encontrando en cada uno de los aspectos que involucran la vida social, las tecnologías de la información se erigen como una herramienta de doble filo que por un lado acorto los caminos en la interacción social, económica y cultural, pero que, por otro, abrió una brecha a los delincuentes cibernéticos, que ahora tienen la posibilidad de hacerlo dese cualquier parte del mundo.

La Relación que existe entre el derecho y la tecnología, es cada día más estrecha y se va entrelazando a raíz de los conflictos y garantías que pueden verse involucradas en el ámbito tecnológico, ya sea usando esta herramienta como medio para cometer delitos del diario vivir, como hurtos, injurias, calumnias, etc. o en el que la información y los datos en constante tránsito, surgen como un bien jurídico objeto de protección legal.

Con los nuevos paradigmas jurídicos que acompañan la tecnología y la informática, surge el planteamiento en cuanto al ámbito la aplicación de las penas, pues podría pensarse en incorporar sanciones penales accesorias distintas a las tradicionales, como por ejemplo la inhabilitación para el ejercicio de derechos y funciones informáticas, restricción que resultaría más eficaz, por el perjuicio que traería el tiempo de la sanción para esta clase de delincuentes, además de tener una función de prevención general de los delitos informáticos.

El delito de interceptación de datos informáticos no es lo necesariamente claro al determinar su descripción típica, ya que como se observó no sólo es necesaria la orden judicial previa a la que alude el tipo, si no que adicionalmente se requiere de

la orden judicial posterior, generando una disparidad con lo que expresamente consagra el articulo 269C del Código Penal Colombiano, ya que este último requisito no se encuentra allí.

A manera de crítica constructiva, la expresión “el que sin orden judicial previa”, contenida en el tipo del 269C, podría relevarse por “el que sin estar legalmente autorizado”, en la medida que la primera expresión ineludiblemente se está advirtiendo de alguna manera al funcionario de Policía Judicial que realiza la interceptación de datos informáticos a cumplir con el control judicial correspondiente, y no a un sujeto indeterminado, que es lo que a priori menciona el tipo penal.

REFERENCIAS

Sentencia C-336 (Corte Constitucional de Colombia 2007).

Sentencia C-334 (Corte Constitucional de Colombia 2010).

alfa-redi.org. (2015). Obtenido de http://www.alfa-redi.org/sites/default/files/articles/files/piacenza_2.pdf

Alonso García, J. (2015). Derecho Penal y redes sociales. Pamplona, España.

Alvarado Carmona, M. A. (2016). *redalyc.org.* Obtenido de https://www.redalyc.org/pdf/5177/517754056019.pdf - Aspectos legales al utilizar las principales redes sociales en Colombia

Alvarez Pardo, Á. (2017). *Derecho Penal y las nuevas Tecnologias.* Universidad de Salamanca.

Arboleda Vallejo, M., & Ruiz Salazar, J. A. (2017). Manual de Derecho Especial.

Beck, U. (1986). *La Sociedad del Riesgo-hacia una nueva normalidad.* Ediiones Paidós Iberica S.A.

Betancur, J. D. (1998). Conceptos Básicos sobre la Tecnología. *Informador Técnico- Universidad EAFIT*.

Carrillo, M. R. (2012). *Corte Interamericana de Derechos Humanos.* Obtenido de https://www.corteidh.or.cr/tablas/r32923.pdf

Cea Jiménez, A. d. (2012). *Los delitos en las redes sociales: aproximación a su estudio y clasificación.* Obtenido de https://gredos.usal.es/bitstream/handle/10366/121119/TFM_CeaJim%E9nez_Delitosenredessociales.pdf;jsessionid=EBC27953CFCD00A5A677E0EB30A8DAE1?sequence=1

Congreso de la República de Colombia. (5 de Enero de 2009). *“Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comun.*

Congreso de la Republica de Colombia. (s.f.). Código de Procediemiento Penal - Ley 906 de 2004.

Congreso de la República de Colombia. (s.f.). Codigo Penal Colombiano. Colombia.

Convenio de Budapest del Consejo de Europa contra la cibercriminalidad. (2001). Obtenido de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Cuervo Álvarez, J. (1999). *Delitos Informáticos: protección penal de la intimidad.* Obtenido de http: //publicaciones.derecho.org/redi/No._06_-_Enero_de_1999/cuervo.

Dahiman, C. W. (1983). La transferencia de la Tecnología, En finanzas y desarrollo.

Escobar, D., & Jimenez, D. (2018). Obtenido de https://repositorio.unibague.edu.co/jspui/bitstream/20.500.12313/1925/1/Trabajo%20de%20grado.pdf

Fernandez, D. A. (2011). *redalyc.org.* Obtenido de https://www.redalyc.org/articulo.oa?id=28220704002

Fiscalía General de la Nación. (2014). Obtenido de - https://www.fiscalia.gov.co/colombia/wp-content/uploads/20170111.pdf

Fiscalia General De La Nación Colombia. (2 de Junio de 2020). *www.fiscalia.gov.co/.* Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Direccionamiento-Estrate%CC%81gico-2020-Covid-19.pdf

Franco Reyes, A. (2017). Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/14511/1/LAS%20REDES%20SOCIALES%20Y%20LOS%20DELITOS%20DE%20INJURIA%20Y%20CALUMNIA%20EN%20COLOMBIA%20%285%29.pdf

Galindo, J. (2015). *EL CONCEPTO DE RIESGO EN LAS TEORÍAS DE ULRICH BECK Y NIKLAS LUHMANN.* Obtenido de https://reader.elsevier.com/reader/sd/pii/S0186602815000262?token=E90716D737E4FD6B83E933EDB46BA7739E9E28C7FAF6D6D96412D4BC53E8FAA2A65027D119FCC8BDC36FC0A164EEB765

Iuris Tantum Revista Boliviana de Derecho. (2016). *scielo.org.* Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572016000100001

Jara Obregon, L., Ferruzola Gómez, E., & Rodriguez López, G. (2014). Obtenido de Delitos a través redes sociales en el Ecuador: una aproximación a su estudio: https://revistas.utp.ac.pa/index.php/id-tecnologico/article/view/1721/html

León Felipe, G. (24 de Septiembre de 2020). *LegalToday.com*. Obtenido de https://www.legaltoday.com/practica-juridica/derecho-penal/penal/delincuencia-en-tiempos-de-coronavirusbr-estafas-y-ciberdelitos-2020-09-24/

Leyva Estupiñan, M. y. (2015). *El bien jurídico y las funciones del Derecho penal - Universidad Externado.* Obtenido de https://revistas.uexternado.edu.co/index.php/derpen/article/view/4482/5125

Loredo González, J., & Ramirez Granados, A. (2013). Obtenido de http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Maillo Fernández, J. (2018). Sistemas Seguros de Acceso y transmisión de Datos. Ediciones de la U.

Manjarrés, I., & Jímenez, F. (2012). Caracterización de los delitos informáticos en Colombia. *Pensamiento Americano*.

Ministerio de las Tecnologias de Informacion y las Comunicaciones. (2020). Obtenido de https://mintic.gov.co/portal/inicio/Sala-de-Prensa/Sabia-Ud-que/2713:Colombia-es-uno-de-los-paises-con--la-regionmas-usuarios-en-redes-sociales-en Colombia.

Naranjo Mesa, V. (2000). *Teoría Constitucional e Instituciones Políticas.* Bogotá: Temis.

Nezeys, B. (1985). Comercio Internacional. España.

NIC Argentina - Dirección Nacional del Registro de Dominios de Internet,. (2017). *nic.ar*. Obtenido de https://nic.ar/es/enterate/novedades/que-es-convenio-budapest

Peña, C. (2016). *palermo.edu.* Obtenido de Universidad de Palermo: https://www.palermo.edu/ingenieria/downloads/pdfwebc&T8/8CyT05.pdf

Periódico El Nuevo Siglo - Colombia. (2020). *El Nuevo Siglo*. Obtenido de https://www.elnuevosiglo.com.co/articulos/05-2020-62-aumentaron-delitos-informaticos-durante-la-cuarentena

Poder Judicial de México. (s.f.). Obtenido de http://www.poderjudicial-gto.gob.mx/pdfs/ifsp_conceptosjuridicosfundamentales-1.pdf

Posada Maya, R. (2017). Obtenido de Los cibercrímenes : Un nuevo paradigma de criminalidad: un estudio del título vii bis del código penal colombiano.: https://elibro.net/es/ereader/usta/118331?page=275

Posada Maya, R. (2017).

Posada Maya, R. (2017). Obtenido de Los cibercrímenes: un nuevo paradigma de criminalidad: un estudio del Título VII bis del Código Penal Colombiano.: https://elibro.net/es/ereader/usta/118331?page=275

Ramirez, O. J. (2009). RIESGOS DE ORIGEN TECNOLÓGICO: APUNTES CONCEPTUALES PARA UNA DEFINICIÓN,. *Revista Luna Azul ISSN 1909-2474*, 89-91.

Sain, G. (2013). Obtenido de El derecho Penal aplicado a los delitos informaticos: Una politica eficiente para el cibercrimen?: http://www.saij.gob.ar/gustavo-sain-derecho-penal-aplicado-delitos-informaticos-una-politica-eficiente-para-cibercrimen-dacf130148-2013-06-18/123456789-0abc-defg8410-31fcanirtcod

Sain, G. (2013). *Revista Pensamiento Penal.* Obtenido de http://www.pensamientopenal.com.ar

Saín, G. (2015). *Revista Pensamiento Penal.* Obtenido de http://www.pensamientopenal.com.ar/doctrina/40877-evolucion-historica-delitos-informaticos

Schwab, K. (2016). Obtenido de http://40.70.207.114/documentosV2/La%20cuarta%20revolucion%20industrial-Klaus%20Schwab%20(1).pdf

Sentencia Condenatoria contra Andres Fernando Sepúlveda (Juzgado Veintidós (22) Penal del Circuito con Funciones de Conocimiento de Bogotá 10 de Abril de 2015).

Tellez Valdéz, J. (2005). *Derecho Informático.* Universidad Nacional de México.

Téllez, V. J. (1997). Derecho Informático. Editorial McGraw Hill, México. Obtenido de Derecho Informático, Editorial McGraw Hill, México, 1997, págs., 105 y ss.

UJAEN.ES. (s.f.). Obtenido de http://www.ujaen.es/investiga/tics_tfg/enfo_cuali.html

Valdés Meza, E. (2009). Obtenido de https://www.u-cursos.cl/derecho/2009/1/D121D0529/2/material_docente/previsualizar?id_material=212108

Vasquez Santamaría, J., & Mesa, A. M. (2012). La Interceptacion de Datos Informáticos entre la licitud y lo delictual. *Lámpsakos*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=4490594